REMARKS

We are enclosing drawings (2 sheets) to replace the ones presently in the application. The replacement drawings are devoid of extraneous markings.

Claims 25-61 are in the application. The examiner has rejected independent claims 25, 36, 37 and 60 and the claims dependent thereon as being obvious for claims 25 and 36 in view of Rosen '518 and Chang '425, for claim 37 in view of Rosen and Chang in combination with Pitroda '038 and Abraham '481, and for claim 60 in view of Rosen and Halter '705. We request withdrawal of these rejections for the reasons set forth below.

To simplify the issues, we will respond in detail to the examiner's rejection of the independent claims 25, 36, 37 and 60, it being understood that the claims dependent thereon should be allowed for the same reasons.

A very detailed description of the Rosen system was provided in our response filed February 24, 2004 and will not be repeated here. We will, however, point out certain critical inaccuracies in the examiner's description of that system as set forth in Part 4 of the current Official Action. These inaccuracies indicate that the Examiner is tailoring the prior art to fit applicant's claims. We submit that when viewed in the context of what the references actually do disclose, it is clear that applicant's claimed invention is not obvious from Rosen and Chang with or without the other references of record and that the rejections of the claims are based on a hindsight application of that prior art.

Since obviousness is measured in the mind of the so-called skilled artisan, we should point out that applicant, Peter Landrock, is an expert in the field of electronic Bills of Lading and cryptology. He has carried out fundamental studies for the European Commission on the feasibility of electronic Bills of Lading. This includes extensive study of the use of, as well as the legal aspects of, Bills of Lading and international trading. In addition, his company was responsible for the first world-wide pilot on electronic Bills of Lading in the project BOLERO, which later was built as a complete commercial solution by SWIFT (the World-Wide Clearing House of Banks) and other partners. As evidence of his expert skills in these fields, suffice it to state here that he was elected President of the International Association of Cryptologic Research (IACR) from 1992 through 1995 and has published a number of papers on cryptology. He was also a key-note speaker at Asiacrypt '93, Eurpocrypt '95 and the IEEE conference at Ulm in 1997 to mention but a few examples of peer recognition around the time of his claimed invention.

Turning to the rejection of claim 25, the examiner states in Part 4, second paragraph of the action that Rosen "shows elements that suggest a 'method of issuing an electronic negotiable document...'[i.e., 'electronic money']. This is clearly meant to suggest that Rosen is including electronic money within his definition of electronic commerce when, in fact, that is not the case. On the contrary, Rosen issues electronic merchandise in the form of tickets in return for money. Nowhere does he contemplate issuing an electronic negotiable document as that term is universally recognized, i.e. documents in the form of cash, bank checks and Bills of Lading. In sum, Rosen does not even remotely

suggest the issuance of electronic money, but rather only non-negotiable merchandise, i.e. in the form of tickets"; see Pat. Col. 4, Line 41.

In the next paragraph of Part 4 of the Action, the examiner states that Rosen "shows elements that suggest 'a unique public-secret key pair for signing and verifying...". In the first place, Rosen does not actually use a public-secret key pair as that term is used in the industry. Rather, Rosen uses symmetric cryptology rather than public-key encryption for transferring a ticket; see Pat. Col 16, Lines 38-39. In symmetric cryptology, both keys are kept secret. Indeed this is clearly the case in the Rosen system. As stated at Rosen Pat. Col. 10, Lines 61 et seq.:

> "The term 'public key' as used here and throughout the specification does not imply that the key is known to the public at large. In this case, for example, the public key is known only to all trusted servers 200 and trusted agents 120 and is sealed within their tamper-proof housings."

In contrast to that, applicant's arrangement relies on asymmetric cryptology involving the use of a public key that is available to all as is clearly evident from the frequent references in the claim language to public and secret keys, i.e. utilizing the well known RSA and DSA algorithms referred to on page 3 of the specification.

Since Rosen's so-called public key is really a private key, that reference cannot possibly suggest "a unique public-secret key pair for signing and verifying", as stated by the Examiner in Part 4 of the action, third paragraph, let alone the creation and storage of such a key pair in tamper resistant document carrier hardware as required by claim 25. On the contrary, we contend that the creation and storage of a public-private key pair in tamper-resistant document carrier hardware is neither taught nor suggested by Rosen.

In the fourth paragraph of Part 4 of the Action, the examiner asserts that Rosen "shows elements that suggest...a document carrier containing...a unique document carrier identifier..." Applicant's claims have been amended to specify tamper-resistant document carrier hardware. We have read the portions of the Rosen patent relied on by the Examiner Part 4 of the action, and find nothing that suggests tamper-proof document carrier hardware, let alone such hardware that contains a unique document carrier identifier. Those patent portions deal with the exchange of electronic merchandise for money. Since Rosen never contemplates a unique document carrier identifier, it is not surprising that he does not disclose or suggest the signing of such an identifier as required in claim 25. Thus while it may be that digital signatures are well known in the art as observed by the Examiner, that is not to say that it is obvious to apply such a signature to a document carrier identifier, particularly when there is no suggestion that such a unique document carrier identifier is even present in Rosen's patented system.

We also point out that claim 25 requires not only the signing of a document carrier identifier (which is not found in Rosen), but also requires a signing of the END and an END identifier. How can it be obvious for Rosen to sign both an END identifier and a unique document carrier identifier when those elements are not present in the Rosen system. Of course, we also deny that the signing of the END itself is obvious from Rosen because Rosen is concerned with merchandise not ENDs.

At the top of page 5 of the Action, the Examiner relies on the Chang reference to disclose a tamper-resistant document carrier. As noted above, the claims in the present application has been amended to specify tamper-resistant document carrier hardware.

We submit that Chang merely discloses public-key encryption to protect data. Nowhere does he describe tamper-resistant document carrier hardware.

But more importantly, we submit that it is not at all obvious to combine Chang and Rosen as proposed by the Examiner because the Rosen system utilizes symmetric cryptology involving two secret keys whereas Chang relies on asymmetric or public-key cryptology. The two systems are incompatible and combining their teachings would involve a wholesale reconfiguration of the Rosen system and the method of operating it. But even as combined, that hypothetical assemblage would still not be the equivalent of applicant's claim method because that assemblage would still not be able to perform the sequence of method steps set forth in claim 25.

To put it another way, since neither the Rosen nor the Chang apparatus has anything to do with electronic negotiable documents as that term is universally recognized, how can any proper combination of those references suggest applicant's method of electronically issuing such a document?

Referring to independent claim 36, that claim is allowable over Rosen and Chang for the same reasons given above for claim 25. Rosen refers to electronic merchandise, i.e. tickets, not to negotiable documents such as money. Moreover, in Rosen there is no negotiating in the sense of applicant's claimed procedure, contrary to the Examiner's suggestion at the bottom of page 8 of the action. In the paragraph bridging pages 8 and 9 of the action, the Examiner asserts that Rosen "shows elements that suggest a 'carrier having its own public-secret key pair'..." As noted above, Rosen's so called public key is really a private key that is not available to the general public.

In the middle of page 9 of the action, the Examiner states that Rosen "shows elements that suggest 'establishing mutual recognition between the seller and the buyer using predetermined protocol between the respective document carriers...[and] aborting the negotiation'..." That language from applicant's claim 36, in fact, refers to "verifying in the seller's document carrier hardware that the negotiability status flag is 'negotiable' and aborting the negotiation if not." We submit that this feature is neither taught nor suggested in Rosen which uses a different procedure not involving a negotiability status flag; see section "Abort and Commit" at Rosen Pat. Col. 13, Line 36.

In fact, Rosen does not teach or suggest the use of a negotiability status flag since he teaches the use of a different procedure which has no use for such a flag. In that part of the action, the Examiner refers to Rosen Col. 6, Lines 26-32 and the elements 58, 84 and 100 of Pat. Fig. 2. However, we respectfully submit that there is no suggestion there that these elements should be used as a negotiability status flag. For example, the description of the "Abort and Commit" procedure at Pat. Col. 13 onward makes no reference whatsoever to these elements.

The combining of the Chang teaching with that of Rosen does not overcome the above noted deficiencies in Rosen. We submit further that Chang does not even suggest the use of tamper-resistant document carrier hardware even if it were obvious to combine those references, which we deny as discussed above.

Turning now to independent claim 37, the same points raised with respect to claims 25 and 36 apply here as well. Rosen concerns electronic merchandise, not to an END. Rosen uses symmetric private key cryptology for encrypting messages (tickets),

whereas claim 37 specifies the use of public key cryptology for an END. The use of symmetric cryptology as opposed to public key cryptology has a major impact on the procedure since with the former, both keys must be kept secret as is the case with Rosen's system, but not according to applicant's claimed invention.

Thus the combining of Chang with Rosen in the rejection of claim 37 is not appropriate because Chang's public key encryption cryptology is not compatible with Rosen's private key encryption cryptology and there is nothing in the references themselves that suggest that they can be so combined. Moreover, since neither of those patented systems is concerned with electronic negotiable documents (ENDS), no proper combination of the two can teach applicant's claimed method for electronically negotiating such a document. And even if those references were combined as proposed, they do not teach the specific method steps recited in claim 37, specifically those involving a serial number counter indicative of the number of times that the END has been negotiated since issue and the incrementing of that counter by one as specified at the end of claim 37.

In rejecting claim 37, the Examiner adds Pitroda to the Rosen/Chang combination. In part 7 of the action on page 22, the Examiner appears to suggest that Pitroda shows elements that suggest a serial number counter indicative of the times that the END has been negotiated. We respectfully submit that this is not the case because the patent passages referred to (Pitroda Col. 15, Lines 58-63 and Col. 16, Lines 39-40) make no reference whatever to a counter and, we submit, neither teach nor suggest a serial number counter indicative of the number of times an END has been negotiated. Pitroda does ap-

pear to refer to a "unique serial number of the UET card" (Pat. Col. 15, Line 62), but the patent make no reference to serial number modifications. Furthermore, for a serial number to be "unique" as specified in the patent, this tends to imply that that number should not be changed (to avoid the risk of collision with the "unique" numbers). Thus there is nothing in Pritroda to teach or suggest incrementing a counter or counting a number of times that an END has been negotiated.

In that same part of the action, the Examiner also appears to assert that Rosen shows elements that suggest verifying in the seller's document carrier that an END, if it has been stored previously in that document carrier, has a different counter value this time and is therefore negotiable. However, nowhere does Rosen refer to a counter or to the use of a counter in the manner claimed in claim 37.

At the bottom of page 25 of the action, the Examiner asserts that Rosen (Figs. 1 and 2) "shows elements that suggest 'sending the public encryption key of the buyer's document carrier to the seller's document carrier, and using it to encrypt the message comprising the END together with the counter, sending that encrypted message to the buyer'." We respectfully deny this because there is nothing whatever in Rosen's Figs. 1 or 2 to either teach or suggest a counter, or encrypting an END together with a counter by any sort of cryptology.

In the rejection of claim 37 at page 26 of the action, the Examiner also relies on Abraham "as suggesting encrypting a 'message comprising the END together with the counter, sending the encrypted message to the buyer...and incrementing the counter by

one'." We respectfully submit that Abraham shows no such thing because Abraham does not, in fact, use a counter to count. As clearly stated at Pat. Col. 5, Lines 13-17:

> "It is not important that the counter actually counts upward in the conventional sense. What is really important is that it change each time a new random number is generated, and that it steps through a very large number of states."

In sum, Abraham does not teach using a counter to count but rather to generate random numbers. No skilled artisan would ever have attempted to combine the Abraham and Rosen teachings, with or without Chang and we further submit that even if such a combination were made, there is nothing in that hypothetical assemblage to either teach or suggest the subject matter of claim 37. Accordingly claim 37 should be allowed.

Finally with respect to claim 60 which stands rejected as being unpatentable over Rosen in view of Halter, aside from the fact that neither Rosen nor Halter is concerned with electronic negotiable documents, the Examiner, in page 40 of the action, appears to acknowledge that Rosen does not explicitly show "the buyer splits the END electronically into two or more parts and then negotiates those parts separately to one or more further buyers, and then states Halter appears to suggest this. We submit, however, that there is absolutely no mention in Halter, and specifically in the passage quoted by the Examiner and accompanying figure, of splitting an END electronically into two or more parts, and no mention of negotiating those parts separately to one or more further buyers. Therefore, one of ordinary skill in the art would never have combined Halter with Rosen as proposed by the Examiner. Moreover even if such a combination were made, there is

nothing in such a combination to either teach or suggest the splitting of an END followed by renegotiating the split parts.

The fact is that none of the references applied against applicant's independent claims, i.e. Rosen, Chang, Pitroda, and Abraham, relates at all to an electronic negotiable document (END) or to the secure issuing and negotiating of same as set forth in any of applicant's independent claim 25, 36, 37, and 60. Therefore, no proper combination of those references can do so.

The remaining claims, being dependent upon one or another of the above independent claims, should be allowed for the same reasons. They are allowable also in specifying additional method steps not taught by the references of record.

In closing, we note that substantially all of the Examiner's observations regarding the references include the phrase "appears to suggest" followed by applicant's claim language. This appears to suggest that the various claim rejections are based on a hindsight analysis of the prior art made possible only after the Examiner has had the benefit of applicant's disclosure. That type of rejection is not compatible with prevailing law.

For the foregoing reasons, this application should be allowed.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,

John F. McKenna
Reg. No. 20,912
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500